NSO Group Used at Least 3 iOS Zero-Click Exploits in 2022: Citizen Lab

Israeli spyware vendor NSO Group used at least three previously unknown iOS zero-click exploits in 2022, according to a new report from Citizen Lab.

NSO Group's Pegasus spyware has often been delivered to targeted iPhones using zero-click and/or zero-day exploits, and while Apple has taken steps to prevent attacks against its customers, NSO's exploit developers continue to find ways to bypass mitigations.

Citizen Lab, a group at the University of Toronto that focuses on human rights and security research, came across the new iOS exploits while investigating malware infections on the iPhones of human rights defenders in Mexico.

One of the new zero-click exploits discovered by Citizen Lab has been named PwnYourHome. This two-step exploit targets HomeKit and iMessage and it was used against iOS 15 and 16 devices starting with October 2022.

Another two-step exploit, which targets the Find My feature and iMessage, has been dubbed FindMyPwn. This zero-click exploit has been used against iPhones running iOS 15 since at least June 2022.

The third, named LatentImage, was seen on only one device and it seems to be the first new exploit used by NSO in 2022.

The FindMyPwn and PwnYourHome exploits were used as zero-days.

Apple was informed about the findings in October 2022 and January 2023. One of the vulnerabilities involved in these attacks is CVE-2023-23529, which Apple fixed in February. It’s unclear what other CVE identifiers have been assigned to the flaws associated with these exploits. The tech giant has patched roughly a dozen iOS zero-days over the past year.

Apple sent out notifications to targeted users in November and December 2022, as well as in March 2023.

NSO Group may have since improved its exploits, but Citizen Lab has not seen the PwnYourHome exploit work against devices that had Apple’s Lockdown Mode feature enabled.

Citizen Lab discovered the new exploits after finding indicators of compromise known to be associated with Pegasus attacks, but the organization has decided not to disclose those indicators as NSO Group might leverage the information to ensure that future attacks are not detected.

Citizen Lab and Microsoft recently detailed the iOS malware developed by an Israel-based spyware vendor named QuaDream. The company, described as a competitor of NSO, is reportedly shutting down, partly due to the latest revelations.

Related: Google, CISA Warn of Android Flaw After Reports of Chinese App Zero-Day Exploitation

Related: □□Apple Patches Exploited iOS Vulnerability in Old iPhones

Related: Citizen Lab Documents Israeli Surveillance Spyware Infections in Spain

NSO Group Used at Least 3 iOS Zero-Click Exploits in 2022: Citizen Lab